WEB APPLICATION FIREWALL MANAGEMENT

FortiWeb Manager Administration Guide

VERSION 5.5.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

May 04, 2016

FortiWeb Manager 5.5.1 Administration Guide

1st Edition

TABLE OF CONTENTS

Introduction

FortiWeb Manager centralizes the configuration of FortiWeb appliances. Its web UI replaces the local interfaces on FortiWeb appliances in your network, allowing you to create, deploy and update their configurations remotely.

Instead of creating a local configuration on a remote FortiWeb, the manager allows you to create a configuration that you can install on one or more FortiWebs. To make changes to a configuration, edit the FortiWeb Manager package (or create a new one) and deploy the updated package to the remote appliance.

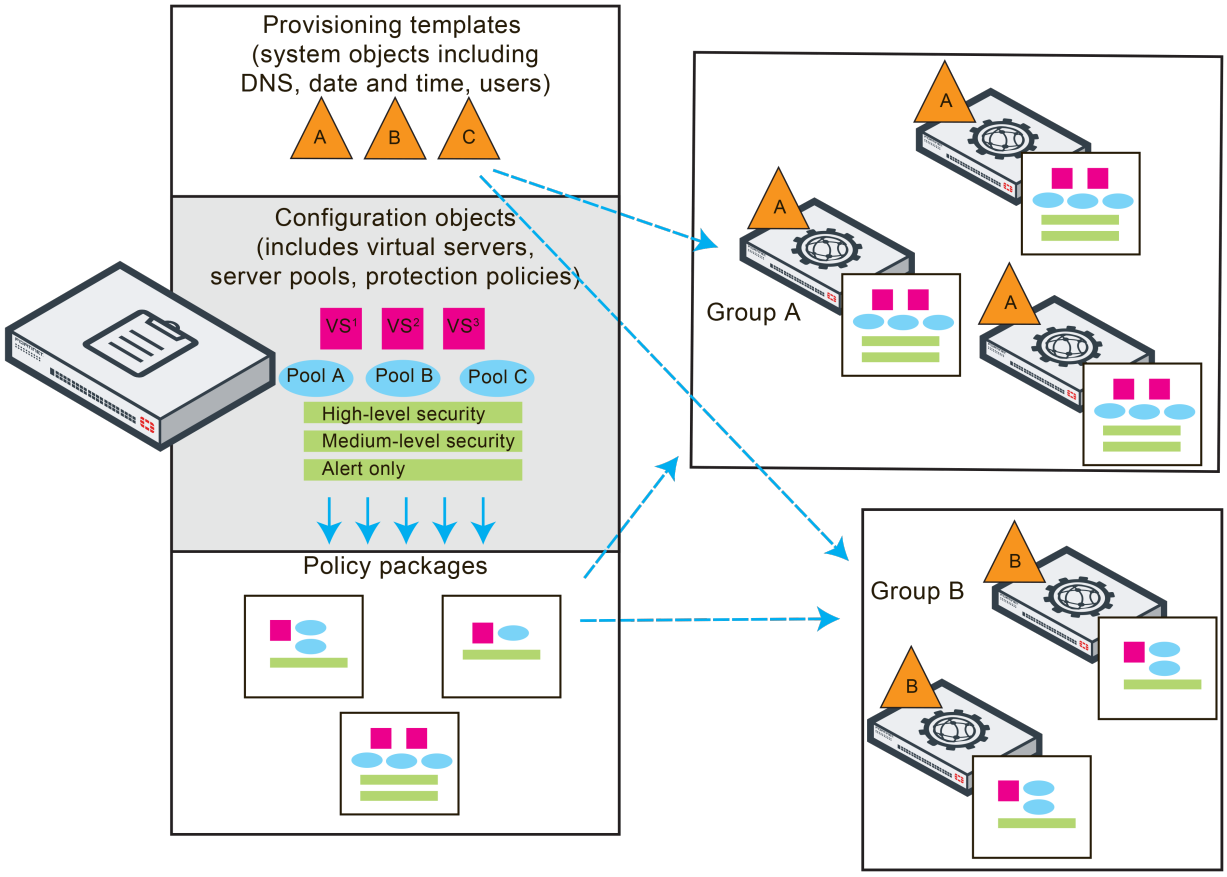
The configuration you install using FortiWeb Manager replaces any default or existing configuration on the remote appliance. However, you can revert to the previous configuration using the installation logs. (See Package Install on page 25 and Templates Assign on page 25.

Using FortiWeb Manager to configure devices

In FortiWeb Manager, FortiWeb configuration is organized in two parts:

- **Provisioning templates** – System objects including DNS, SNMP, and security settings. In most cases, you set these settings during an initial deployment and do not update them often.
- **Policy packages** – Contain one or more policies you create using configuration objects such as virtual servers, server pools, and web protection policies. You create these configuration objects separately and add them to the policies found in packages as needed.

  To update configurations you installed using policy packages, edit the configuration objects and policies as needed, and then install the updated package.



Web UI organization

You perform tasks that configure remote FortiWeb devices using the following two tabs:

- **Device Manager tab** – Allows you to perform the following provisioning tasks:
  - Create a list of FortiWeb appliances available for configuration. To help you organize your devices, you can add a device to a group when you add it.
  - Change an individual configuration setting on an appliance.
  - Create and assign reusable system templates that contain values for the settings that are most commonly used when you provision an appliance, including DNS, SNMP, and security settings.
  - Upload firmware and data analytics definitions files and use the uploaded files to upgrade the FortiWeb appliances in a group.
- **Policy & Objects tab** – Allows you to perform the following policy creation and installation tasks:
  - Create configuration objects such as virtual servers, server pools, and web protection profiles.
  - Create or update policy packages. You create the package policies using the pre-built configuration objects.
  - Install the policy packages on one or more FortiWeb appliances.

The FortiWeb Manager web UI also has a **System Settings tab** that allows you to monitor FortiWeb Manager and to perform tasks such as user management and high availability configuration.

What's new

The list below contains new or changed features for FortiWeb Manager version 5.4 and later.

FortiWeb Manager 5.5 Patch 1

- **FortiWeb 5.5 Patch 3 support** — FortiWeb Manager 5.5.1 supports FortiWeb 5.5.3 only. It allows you to configure all new and enhanced functionality introduced with FortiWeb 5.5.3.
- **Backup and restore** — You can now back up your FortiWeb Manager configuration to a local location or FTP server and use the backed-up file to restore the configuration.

  See Backup & restore on page 18 and FTP Backup on page 18.
- **Read-only administrators** — You now configure an administrator with Read-Write or Read Only access.

  See Administrators on page 17.
- **System time enhancements** — For the system time, you can now select any time zone, synchronize to an NTP server, and automatically adjust for daylight saving time.

  See System Time on page 19.
- **Configure network interfaces using the web UI** — You can now use the web UI to configure the FortiWeb Manager network interfaces.

  See Interface on page 12 and Static Route on page 13.
- **Amazon Web Services (AWS) support** — FortiWeb Manager is now available as an Amazon Machine Image (AMI) for AWS deployment.

FortiWeb Manager 5.5

- **FortiWeb 5.5 Patch 1 support** — FortiWeb Manager 5.5.1 supports FortiWeb 5.5.1 only. It allows you to configure all new and enhanced functionality introduced with FortiWeb 5.5.1.
- **Upgrading gateways**
  - **Upgrade for multiple gateways** — You can now use uploaded firmware and data analytics definitions files to upgrade all FortiWeb appliances in a group in a single operation. The group upgrade operation generates a message in the FortiWeb Manager event log.
  - **Automatic configuration updates** — When it upgrades a gateway, FortiWeb Manager now also attempts to update the gateway configuration to match the features of the newer firmware version. It deletes configurations that it cannot successfully update.
- **Support for Hyper-V** — You can now deploy FortiWeb Manager on the Microsoft Hyper-V hypervisor.

FortiWeb Manager 5.4.1

- **High Availability** — You can group multiple FortiWeb Manager VM appliances together as a high availability (HA) cluster. HA for FortiWeb Manager uses the same configuration settings as HA for FortiWeb appliances, except for the physical port monitoring options.

  See HA on page 13.

- **FortiWeb 5.4.1 support** — FortiWeb Manager supports all new and enhanced functionality introduced with FortiWeb 5.4.1.
  - **SNMP version 3 support** — When you use the Device Manager tab to configure an SNMP community, you can now enable the traps for SNMP v3 instead or in addition to SNMP v1 and v2c.
  - **Policy Sessions widget** — The Policy Sessions widget on the Status dashboard now displays counts of the current connections and connections per second by policy.
- **Real Time Monitor widget** — You can now view the Real Time Monitor widget when you use the Device Manager tab to access a remote appliance's Status Dashboard.
- **Logging**
  - **Template assign and package install logs** — The new logs generate an entry each time you assign a template or install a package. Each entry includes a record of the previous configuration and information such as the template or package name, the device name, and the time of installation. You can use this entry to revert to the previous configuration or download the current or previous installation for troubleshooting purposes.

    See Package Install on page 25 and Templates Assign on page 25.
  - **Event Log** — On the System Settings tab, go to **Logs > Event** to view a record of user actions such as login, logout, add or delete user, and change password.

    See Event on page 26.
- **3000E & 4000E support** — FortiWeb Manager now supports the additional settings used by the FortiWeb 3000E and 4000E models.

FortiWeb Manager 5.4

- **FortiWeb Manager-VM** — The standalone FortiWeb Manager-VM replaces the central management component that was available in some earlier releases of FortiWeb.

  This new central management tool is not available as an appliance-based product and does not include FortiWeb.
- **Enhanced web UI** — The new web UI has tabs and specialized menus that divide management tasks into provisioning, individual setting updates, and policy creation and installation.
- **Device management tab** — The new Device Manager tab allows you to organize your FortiWeb appliances into groups, change individual appliance configuration settings, and provision a FortiWeb by creating and applying a template.
- **Policy & Objects tab** — The new Policy & Objects tab allows you to upload the FortiWeb policies using reusable packages. You create these packages using configuration objects such as virtual servers, server pools, and web protection profiles. You can create, save, and update both the packages and the objects as needed, and install or reinstall them as needed to apply the policies to multiple devices.
- **Cascading and right-click menus** — When you select an appliance on the Device Manager tab, you can use the **Menu** option to open a cascading menu. This menu allows you to navigate to a specific set of configuration settings quickly. You can right-click device, device group, and policy items in the navigation tree to add new items.
- **Base and unlimited licenses** — New licenses remove the 15-day limit of the evaluation license and allow you to manage either 10 or an unlimited number of FortiWeb devices.

Installation

FortiWeb Manager is a version of FortiWeb-VM that you can deploy on the following hypervisors:

- VMware vSphere ESXi
- Microsoft Hyper-V

For detailed instructions for installing the FortiWeb Manager virtual machine, see the *FortiWeb-VM Installation Guide*.

Software requirements

FortiWeb Manager manages devices running FortiWeb 5.5.1 only.

The web UI works with the following browser versions:

- Internet Explorer 10 or 11
- Firefox 25 or 26
- Chrome 26, 30, 31

Uploading the license

By default, FortiWeb Manager is installed with an evaluation license that allows you to configure 1 FortiWeb.

To continue to use the product after 15 days have passed, or to configure additional gateways, one of the following licenses is required. Neither license has an expiry date:

- **Base** – Add up to 10 devices.
- **Unlimited** – No limit to the number of devices you can add.

You upload the base and unlimited licenses using the CLI. For instructions for configuring access to the CLI, see the *FortiWeb-VM Installation Guide*.

To upload a FortiWeb Manager license

1. Log in to the CLI using admin and enter the following command:

   ```
   generate computerid
   ```

2. FortiWeb returns a 16-character code. For example:

   ```
   3FFWH-QS01H-8TVEW-CN6JE
   ```

3. Go to support.fortinet.com and log in.
4. Click **Asset > Register/Renew**.
5. Enter your license registration code, and then click **Next**.

6. Enter the computer ID you generated earlier, and then click **Next**.
7. Complete any remaining steps in the registration wizard.

   The wizard generates a license key. For example:

   ```
   66KW6E7PHP2BPN6TDI4W83V7S9ZV182EITMZ5NOAE2ZMZDISW5Y2GVIV4UE8NU4Q
   ```

8. Log in to the CLI using admin and enter the following command:

   ```
   execute register license <license_key>
   ```

   where `<license_key>` is the key provided by the support site.

   After the virtual machine restarts automatically, full FortiWeb Manager functionality is available.

Accessing the web UI

Accessing the FortiWeb Manager web UI is similar to accessing the FortiWeb web UI: in your web browser, enter the IP address of the network interface that you have configured with administrative access .

For detailed instructions for configuring access to the web UI, see the *FortiWeb-VM Installation Guide*.

System settings

You use the System Settings tab to monitor FortiWeb Manager and to perform tasks such as user management and high availability configuration.

Status

The system status dashboard has some of the same widgets as the FortiWeb web UI.

Like the FortiWeb dashboard, on the System Information widget, you can click **Update** to upload a new version of the FortiWeb Manager firmware.

Interface

The Interface options allow you to configure the network interfaces and change their status.

To access the Interface options, go to **System > Network > Interface**.

A network interface's Status column displays whether the interface is configured to receive or emit packets. Click **Bring Up** or **Bring Down** to change the status.

Link Status indicates the detected physical link status.

To edit a network interface, in the appropriate row, under Action, click **Edit**.

Interface settings

Setting name	Description
Name	The name and media access control (MAC) address of this network interface. The name indicates the associated physical interface (for example, port2).
Addressing mode	Specify whether FortiWeb Manager acquires an IPv4 address for this network interface using DHCP.
IPv4/Netmask	Enter the IP address and subnet mask, separated by a forward slash (/). For example, `192.0.2.2/24`. Ensure the IP address is on the same subnet as the network the interface connects to. Two network interfaces cannot have IP addresses on the same subnet.
Description	Optionally, enter information about the interface.

Static Route

The Static Route options allow you to configure a gateway for FortiWeb Manager.

Static routes direct traffic exiting FortiWeb Manager based on the packet's destination — you can specify through which network interface a packet leaves and the IP address of a next-hop router that is reachable from that network interface. Routers are aware of which IP addresses are reachable through various network pathways and can forward those packets along pathways capable of reaching the packets' ultimate destinations. Your FortiWeb Manager itself does not need to know the full route, as long as the routers can pass along the packet.

You configure at least one static route that points to a router, often a router that is the gateway to the Internet. You configure multiple static routes if you have multiple gateway routers (for example, each router receives packets destined for a different subset of IP addresses), redundant routers (for example, redundant Internet/ISP links), or other special routing cases.

However, in most cases, you configure only one route: a default route.

To add a route, go to **System > Network > Static Route**, and then click **Create**.

Static Route settings

Setting name	Description
Destination IP/Mask (IPv4/IPv6)	Enter the destination IP address and network mask of packets that use this static route, separated by a slash (/). Enter `0.0.0.0/0.0.0.0` or `::/0` to create a default route that matches the `DST` field in the IP header of all packets.
Gateway (IPv4/IPv6)	Enter the IP address of the next-hop router to which FortiWeb Manager forwards packets that match **Destination IP/Mask (IPv4/IPv6)**. Ensure that this router knows how to route packets to the destination IP addresses or forward packets to another router with this information. For a direct Internet connection, this is the router that forwards traffic towards the Internet, and could belong to your ISP.
Interface	Select the network interface through which FortiWeb Manager routes the packets that match **Destination IP/Mask (IPv4/IPv6)** to the next-hop router.

HA

You can group multiple FortiWeb Manager appliances together as an **active-passive** high availability (HA) cluster. HA for FortiWeb Manager uses the same configuration settings as HA for FortiWeb appliances, except for the physical port monitoring options.

FortiWeb Manager HA is **active-passive**: one appliance is the active appliance (also called the primary, main, or master) and the other appliance is a passive standby (also called the secondary, or slave), which assumes the role of the active appliance only if the active appliance fails.

This guide provides basic information about the FortiWeb Manager HA settings. See the *FortiWeb Administration Guide* for detailed HA cluster information, including:

- An overview of HA heartbeat & synchronization mechanisms and behavior
- How HA chooses the active appliance
- HA cluster topology
- Step-by-step configuration
- Troubleshooting

HA requirements

- Two identical FortiWeb Manager appliances (that is, VMs running the same firmware version).
- A valid license for all cluster members. You cannot configure HA with trial licenses.
- vNetwork interfaces that carry heartbeat and synchronization traffic are configured to operate in promiscuous mode and accept MAC address changes.
- Cluster members have the same number of ports and are configured with the same amount of memory and vCPUs.
- Redundant network topology: if the active appliance fails, physical network cabling and routes can redirect web traffic to the standby appliance.
- At least one port on both HA appliances is connected directly, via crossover cables, or through switches.

HA settings

Setting name	Description
Configured HA mode	Select **Active-Passive** to configure this FortiWeb Manager to an HA cluster.
Group-name	Enter a name that identifies the HA pair. This setting is optional, and does not affect HA function. The maximum length is 35 characters.
Device Priority	Type the priority for this appliance when the HA feature selects the main appliance in the HA pair. The appliance with the lowest value has the highest priority. This setting is optional. The valid range is 0 to 9. The default is 5. When **Override** is disabled, uptime is more important than this setting when the HA feature selects the primary appliance.
Override	Enable to make **Device Priority** a more important factor than uptime when the HA feature selects the main appliance.

Setting name	Description
HA Member Group ID	Enter a number that identifies the HA pair. **Ensure that both members of the HA pair have the same group ID.** If there is more than one HA pair on the same network, ensure each HA pair has a different group ID. Changing the group ID changes the cluster's virtual MAC address. The valid range is 0 to 63. The default value is 0.
Detection Interval	Enter the number of 100-millisecond intervals in each pause between heartbeat packets that the one cluster member sends to the other member. This is also the amount of time that a FortiWeb Manager appliance waits before expecting to receive a heartbeat packet from the other appliance. The HA feature synchronizes this setting between the main appliance and standby appliance. The valid range is 1 to 20 (that is, between 100 and 2,000 milliseconds). **Note:** Although this setting is synchronized between the main and standby appliances, configure both appliances with the same **Detection Interval** to prevent a failover from occurring before the initial synchronization.
Heartbeat Lost Threshold	Enter the number of times one of the HA appliances retries the heartbeat and waits to receive HA heartbeat packets from the other HA appliance before it assumes that the other appliance has failed. The HA feature synchronizes this part of the configuration between the main appliance and standby appliance. In most cases, you do not need to change this setting. Exceptions include: • Increase the failure detection threshold if the HA feature detects a failure when none has actually occurred. For example, during peak traffic times, if the main appliance is very busy, it might not respond to heartbeat packets in time, and the standby appliance assumes that the main appliance has failed. • Reduce the failure detection threshold or detection interval if administrators and HTTP clients have to wait too long before they can connect through the main appliance, resulting in noticeable down time. The valid range is from 1 to 60. **Note:** Although this setting is synchronized between the main and standby appliances, configure both appliances with the same **Heartbeat Lost Threshold** to prevent a failover before the initial synchronization.

Setting name	Description
ARP Packet Numbers	Enter the number of times that the FortiWeb Manager appliance broadcasts extra address resolution protocol (ARP) packets when it takes on the main role. (Even though a new NIC has not actually been connected to the network, FortiWeb Manager does this to notify the network that a new physical port has become associated with the IP address and virtual MAC of the HA pair.) This is sometimes called “using gratuitous ARP packets to train the network,” and can occur when the main appliance is starting up, or during a failover. Also configure **ARP Packet Interval**. In most cases, you preserve the default value for this setting. Exceptions include: • Increase the number of times the main appliance sends gratuitous ARP packets if your HA pair takes a long time to fail over or to train the network. Sending more gratuitous ARP packets can help the failover to happen faster. • You want reduce the amount of traffic produced by a failover. Because gratuitous ARP packets are broadcast, sending them may generate a large amount of network traffic. As long as the HA pair still fails over successfully, you could reduce the number of times gratuitous ARP packets are sent. The valid range is 1 to 16.
ARP Packet Interval	Enter the number of seconds the HA feature waits between each broadcast of ARP packets. In most cases, you preserve the default value of this setting. Exceptions include: • Decrease the interval if your HA pair takes a long time to fail over or to train the network. Sending ARP packets more frequently can help the failover to happen faster. • You want reduce the amount of traffic produced by a failover. Because gratuitous ARP packets are broadcast, sending them may generate a large amount of network traffic. As long as the HA pair still fails over successfully, you could reduce the number of times gratuitous ARP packets are sent. The valid range is from 1 to 20.

Setting name	Description
Heartbeat Interface	Select one or more ports on this appliance that the main and standby appliances use to send heartbeat signals and synchronization data to each other (that is, the HA heartbeat link). Connect this port to the same port number on the other member of the HA cluster. For example, if you select **port3** for the primary heartbeat link, connect port3 on **this** appliance to port3 on the **other** appliance.) Select at least one heartbeat interface on each appliance in the HA cluster. You cannot re-use ports that currently have an IP address assigned for other purposes as a heartbeat link. **Tip:** If enough ports are available, you can select both a primary heartbeat interface and a secondary heartbeat interface on each appliance in the HA pair to provide heartbeat link redundancy. (You cannot use the same port as both the primary and secondary heartbeat interface on the same appliance, as this is incompatible with the purpose of link redundancy.) **Note:** If a switch is used to connect the heartbeat interfaces, the heartbeat interfaces must be reachable by Layer 2 multicast.

HA Status

To determine which appliance currently has the role of the main appliance, on the System Settings tab, click **Status**. The **System Information** widget displays whether the appliance is operating as the main or standby appliance.

Administrators

The Administrators options allow you to create an administrator account, specify the method it uses to log in to FortiWeb Manager, and assign its access level. For local users, you also use these options to assign and change account passwords.

To access the Administrators options, go to **System > Admin > Administrators**.

Administrator accounts are either local users who log in with a password that you assign in the Administrator options, or a remote user who authenticates via an LDAP or RADIUS server.

To associate an administrator account with a remote server, first create the remote server query and add to an Admin Group. Then, use the administrator account configuration to select the Admin Group that contains the remote server query to use.

For information on creating LDAP or RADIUS queries, see Remote Server (LDAP and RADIUS) on page 21.

For information on creating administrative groups, see Admin Group on page 20.

Administrators settings

Setting name	Description
Name	Enter a name that identifies the administrator account.
Type	Select the type of user: • **Local User** — The account logs in using the name and password specified in the FortiWeb Manager Administrators settings. • **Remote User** — The account logs in via a remote server query. The query to use is a member of the admin group specified by **Admin User Group**.
Password/ Confirm Password	Specify the password the administrator uses to log in to FortiWeb Manager. Available only when **Type** is **Local User**.
Admin User Group	Select the group that contains the LDAP or RADIUS query the account uses to log in to FortiWeb Manager. For information on creating administrative groups, see Admin Group on page 20. Available only when **Type** is **Remote User**.
Access Profile	Specify whether the account can create, edit, or delete FortiWeb Manager configuration items (**Read-Write**) or only view the configuration (**Read Only**).

Backup & restore

To access the backup and restore options, go to **System > Maintenance > Backup & Restore**.

The backup option allows you to export a copy of the FortiWeb Manager configuration as a gzip compressed tar archive file. The download task is handled by your web browser.

The restore option allows you to restore or replace your FortiWeb Manager configuration with the configuration stored in an backup archive file.

Alternatively, you can export the backup file to an FTP server, either manually or automatically at a scheduled time. See FTP Backup on page 18.

FTP Backup

The FTP backup option allows you to export a copy of the FortiWeb Manager configuration as a gzip compressed tar archive file to an FTP or SFTP server, either manually or automatically at a scheduled time.

To add a one-time or scheduled FTP backup, go to **System > Maintenance > FTP Backup** and then click **Create**.

To restore the configuration, move or copy the backup archive file from the FTP server to local storage, and then go to **System > Maintenance > Backup & Restore** to access the restore option.

You can also export the backup file manually, to local storage. See Backup & restore on page 18.

FTP Backup settings

Setting name	Description
Name	Enter a name that identifies the FTP backup.
FTP Protocol	Select whether to connect to the server using FTP or SFTP.
FTP Server	Enter either the IP address or fully qualified domain name (FQDN) of the server.
FTP Directory	Enter the directory path on the server where you want to store the backup file.
FTP Authentication	Enable if the server requires that you provide a user name and password for authentication, rather than allowing anonymous connections.
FTP User	Enter the user name that the FortiWeb appliance will use to authenticate with the server. Displayed only if you select **FTP Authentication**.
FTP Password	Enter the password the FTP user account uses. Displayed only if you select **FTP Authentication**
Schedule Type	Select either: • **Now** — Initiate the backup immediately. • **Daily** — Schedule a recurring backup for a specific day and time of the week.
Days	Select the specific days when you want the backup to occur. Available only when **Schedule Type** is **Daily**.
Time	Select the specific hour and minute of the day when you want the backup to occur. Available only when **Schedule Type** is **Daily**.

System Time

You can set the FortiWeb Manager clock manually or by synchronizing it with a Network Time Protocol (NTP) server. The System Time settings also allow you to select an appropriate time zone.

System Time settings

Setting name	Description
System Time	Displays the system time when you accessed the settings. Click **Refresh** to see the current system time.
Time Zone	Select the time zone where FortiWeb Manager is located.
Automatically adjust clock for daylight saving changes	Select to configure FortiWeb Manager to automatically adjust its own clock when the specified time zone changes between daylight saving time (DST) and standard time.
Set Time	Select and click the field to choose a specific date and time.
Synchronize with NTP Server	Select to set the system time using the specified Network Time Protocol (NTP) server.
Server	Enter the IP address or domain name of an NTP server or pool (for example, `pool.ntp.org`). To find an NTP server that you can use, go to http://www.ntp.org. Available only when **Synchronize with NTP Server** is selected.
Sync Interval	Enter how often in minutes FortiWeb Manager synchronizes its time with the NTP server. For example, enter 1440 to synchronize FortiWeb Manager with the time server once each day. Available only when **Synchronize with NTP Server** is selected.

Admin Group

The Admin Group settings allow you to associate an LDAP or RADIUS server query with an administrator account. The administrator can then log in to FortiWeb Manager via the associated server.

To associate an LDAP or RADIUS server query with an administrator account, first create the remote server configuration and add to an Admin Group. Then, use the administrator account configuration to select the Admin Group that contains the remote server configuration to use.

For information on creating LDAP and RADIUS queries, see Remote Server (LDAP and RADIUS) on page 21.

For information on creating administration accounts, see

To create an admin group and add an LDAP or RADIUS server configuration to it

Go to **User > User Group > Admin Group**, and then click **Create**.

Enter a name for the group, and then click **OK**.

In the row for the group you just created, click **Edit**.

Click **Create**.

For User Type, select the type of authentication to use.

For Name, select the name of an LDAP or RADIUS query.

For information on creating LDAP or RADIUS queries, see Remote Server (LDAP and RADIUS) on page 21.

Click **OK**.

Remote Server (LDAP and RADIUS)

The Remote Server options allow you to configure communication between FortiWeb Manager and an LDAP server, a RADIUS server, or both.

To associate an LDAP or RADIUS server configuration with an administrator account, you first add the remote server configuration to an Admin Group. Then, use the administrator account configuration to select the Admin Group that contains the remote server configuration to use. The administrator can then log in to FortiWeb Manager via the associated server.

For information on creating administrative groups, see Admin Group on page 20.

For information on creating administration accounts, see

To create an LDAP query, go to **User > Remote Server > LDAP Server**, and then click **Create**.

To create a RADIUS query, go to **User > Remote Server > RADIUS Server**, and then click **Create**.

LDAP Server settings

Setting name	Description
Name	Enter a name that identifies the LDAP communication configuration.
Server IPv4/IPv6	Enter the IP address of the LDAP server.
Server Port	Enter the LDAP listening port number. The default port number is determined by the value of Secure Connection. In most cases, port 389 is used for non-secure connections or for STARTTLS-secured connections, and port 636 is used for SSL-secured (LDAPS) connections.

Setting name	Description
Common Name Identifier	Enter the identifier for the common name (CN) attribute (also called the CNID) to use as the user name. The identifier is often `cn` or `uid`, but varies according to your LDAP directory's schema. For Active Directory, it is often the attribute `sAMAccountName`. For example, for the default OpenLDAP directory that uses the following user object, the CNID is `uid`: uid=hlee,cn=users,dc=example,dc=com
Distinguished Name	Enter the Base DN from which the LDAP query starts. This DN is the full path in the directory to the user account objects. Examples: ou=People,dc=example,dc=com cn=users,dc=example,dc=com
Bind Type	Select one of the following LDAP query binding styles: • **Simple** — Bind using the client-supplied password and a bind DN assembled from the **Common Name Identifier**, **Distinguished Name**, and the client-supplied user name. • **Regular** — Bind using a bind DN and password that you configure in **User DN** and **Password**. • **Anonymous** — Do not provide a bind DN or password. Instead, perform the query without authenticating. Select this option only if the LDAP directory supports anonymous queries.
User DN	Enter the bind DN of an LDAP user account with permissions to query the **Distinguished Name**. For example: cn=FortiWebA,dc=example,dc=com For Active Directory, the UPN (User Principle Name) is often used instead of a bind DN (for example, `user@domain.com`). The maximum length is 255 characters. This field can be optional if your LDAP server does not require FortiWeb Manager to authenticate when it performs queries. Available only when **Bind Type** is **Regular**.

Setting name	Description
Password	Enter the password for the specified User DN. This field can be optional if your LDAP server does not require FortiWeb Manager to authenticate when it performs queries. Available only when **Bind Type** is **Regular**.
Filter	Enter an LDAP query filter string that filters the query's results based on any attribute in the record set. For example: (&(|(objectClass=user)(objectClass=group)(objectClass=publicFolder))) This filter improves the speed and efficiency of the queries. For syntax, see an LDAP query filter reference. If you do not want to exclude any accounts from the query, leave this setting blank. The maximum length is 255 characters. Available only when **Bind Type** is **Regular**.
Group Authentication	Specifies whether only members of the LDAP group specified by **Group DN** can authenticate. Users that are not members of that group are not allowed to authenticate. Also configure **Group Type** and **Group DN**. This option appears only when **Bind Type** is **Regular**.
Group Type	Select the schema of your LDAP directory: • **OpenLDAP** — The directory uses a schema where each user object's group membership is recorded in the `gidNumber` attribute . This is usually an OpenLDAP directory, or another directory where the object class is `inetOrgPerson` or `posixAccount`. • **Windows-AD** — The directory uses a schema where each user object's group membership is recorded in the `memberOf` attribute. This is usually a Microsoft Active Directory server. • **eDirectory** — The directory uses a schema where each user object's group membership is recorded in the `groupMembership` attribute. This is usually a Novell eDirectory server. Group membership attributes may have different names depending on the LDAP directory schemas. The FortiWeb appliance uses the group membership attribute that matches your directory's schema when querying the group DN. Available only when **Bind Type** is **Regular** and **Group Authentication** is enabled.

Setting name	Description
Group DN	Enter the value of the group membership attribute that query results must have in order to be able to authenticate. Your directory's schema determines which value you use. It can be distinguished name such as `ou=Groups,dc=example,dc=com` or a group ID (GID) such as 100. Available only when **Bind Type** is **Regular** and **Group Authentication** is enabled.
Secure Connection	Select to connect to the LDAP server using an encrypted connection. Also specify **Protocol**.
Protocol	Select which secure LDAP protocol to use: • **LDAPS** • **STARTTLS** Available only if **Secure Connection** is enabled.

RADIUS Server settings

Setting name	Description
Name	Enter a name that identifies this RADIUS communication configuration.
Server IPv4/IPv6	Enter the IP address of the primary RADIUS server.
Server Port	Enter the number of the primary RADIUS server listening port. The default port number is 1812.
Server Secret	Enter the RADIUS server secret key for the primary RADIUS server. The primary server secret key should be a maximum of 16 characters in length.
Secondary Server IPv4/IPv6	Enter the IP address of the secondary RADIUS server, if applicable.
Secondary Server Port	Enter the number of the secondary RADIUS server listening port. The default port number is 1812.
Secondary Server Secret	Enter the RADIUS server secret key for the secondary RADIUS server. The primary server secret key should be a maximum of 16 characters in length.
Authentication Scheme	Do one of the following: • Select **DEFAULT** to authenticate with the default method. The default method uses PAP, MS-CHAP-V2, and CHAP, in that order. • Select **MS-CHAP-V2**, **CHAP**, **MS-CHAP**, or **PAP**.

Setting name	Description
NAS IP	Enter the NAS IP address and Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, FortiWeb Manager uses the IP address that it uses to communicate with the RADIUS server.

Logs

Package Install

Each time you install a policy package to a device, FortiWeb Manager adds a new entry to the Package Install log. You can use this log to undo the package installation or download a copy of the current or previous configuration for troubleshooting or backup.

Whenever you install a package, FortiWeb Manager performs a complete backup of the existing configuration. This configuration is the Original Configuration in the Package Install log.

Column name	Description
Package Name	The name of the package in FortiWeb Manager.
Device Name	The name of the device where the package was installed.
Install Time	The time that the package was installed.
Log Name	Click the value to download the configuration that FortiWeb Manager installed.
Original Configuration	Click the value to download the configuration that FortiWeb Manager replaced with the policy package specified by **Log Name**.
Comment	Displays any comment you added when you installed the policy package.
Action	Click **Revert** to re-install the configuration that FortiWeb Manager backed up (saved as the Original Configuration file) before it installed the new policy package. Click **Delete** to remove this entry from the **Package Install** log.

Templates Assign

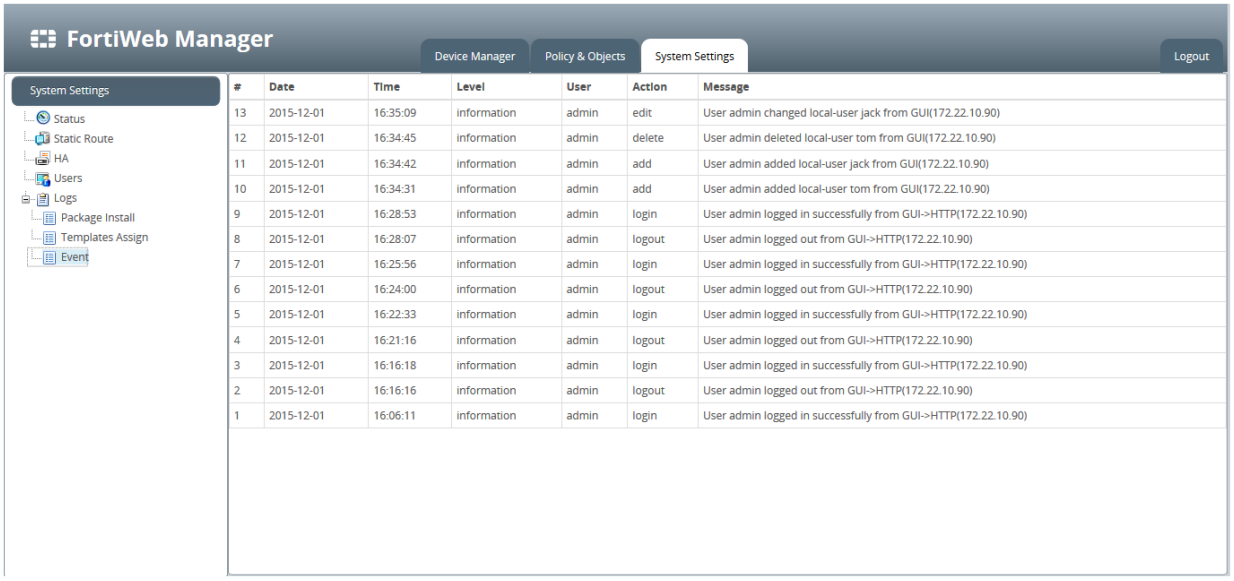
Each time you assign a system template to a device, FortiWeb Manager adds a new entry to the Templates Assign log. You can use this log to undo the template assignment or download a copy of the current or previous settings for troubleshooting or backup.

Whenever you assign a template, FortiWeb Manager performs a complete backup of the existing configuration. This configuration is the Original Configuration in the Templates Assign log.

Column name	Description
Template Name	The name of the system template in FortiWeb Manager.
Device Name	The name of the device the template was assigned to.
Assign Time	The time that the template was assigned.
Log Name	Click the value to download the template that FortiWeb Manager assigned.
Original Configuration	Click the value to download the configuration that FortiWeb Manager replaced with the template specified by **Log Name**.
Action	Click **Revert** to revert to the template configuration values that FortiWeb Manager backed up (saved as the Original Configuration file) before it assigned the new template. Click **Delete** to remove this entry from the **Templates Assign** log.

Event

On the System Settings tab, go to **Logs > Event** to view a record of user actions such as login, logout, add or delete user, and change password.



Add, configure, and provision devices (Device Manager tab)

Add a group

Prepare to add devices to your FortiWeb Manager by creating device groups. These groups allow you to organize your devices in the navigation tree.

To add a group

On the Device Manager tab, click **Add Group** and then complete the following settings:

Name	The name for the FortiWeb Manager device group.
Description	An optional description for the group (for example, a description of its geographic location).

Add a device

Before you add a FortiWeb device to your FortiWeb Manager configuration, ensure that it has the following local configuration:

- The FortiWeb is running the required firmware version. See Software requirements on page 9.
- A network interface that is configured with an IP address that FortiWeb Manager can reach and allows HTTPS connections. (FortiWeb Manager uses HTTPS port 90 to communicate with devices.)
- An administrator account that can access the configuration areas you want to edit using FortiWeb Manager. This account can be `admin`.

Because you specify the group that a device belongs to when you add a device, it is helpful to create the group you want the device to belong to before you add the device.

To add a device

On the Device Manager tab, click **Add Device** and then complete the following settings:

Name	The name for the device in the FortiWeb Manager configuration.
IP Address	The IP address that FortiWeb Manager can use to to communicate with the device.
User Name	The name of an administrator account on the device that can access the configuration areas you want to edit using FortiWeb Manager.

Password	The password that corresponds to the specified **User Name**.
Add to Groups	• **None** – The device does not belong to a group. • **Specific** – The device belongs to the FortiWeb Manager group specified by **Group**.
Group	The FortiWeb Manager group the device belongs to. Available only if **Add to Groups** is **Specific**.
Description	An optional description for the device (for example, a description of its physical location).

Access device configuration

Use the **Devices & Groups** navigation menu to access the configuration settings for an individual device. You can also use this menu to access the status dashboard information and other tasks you perform using the FortiWeb web UI.

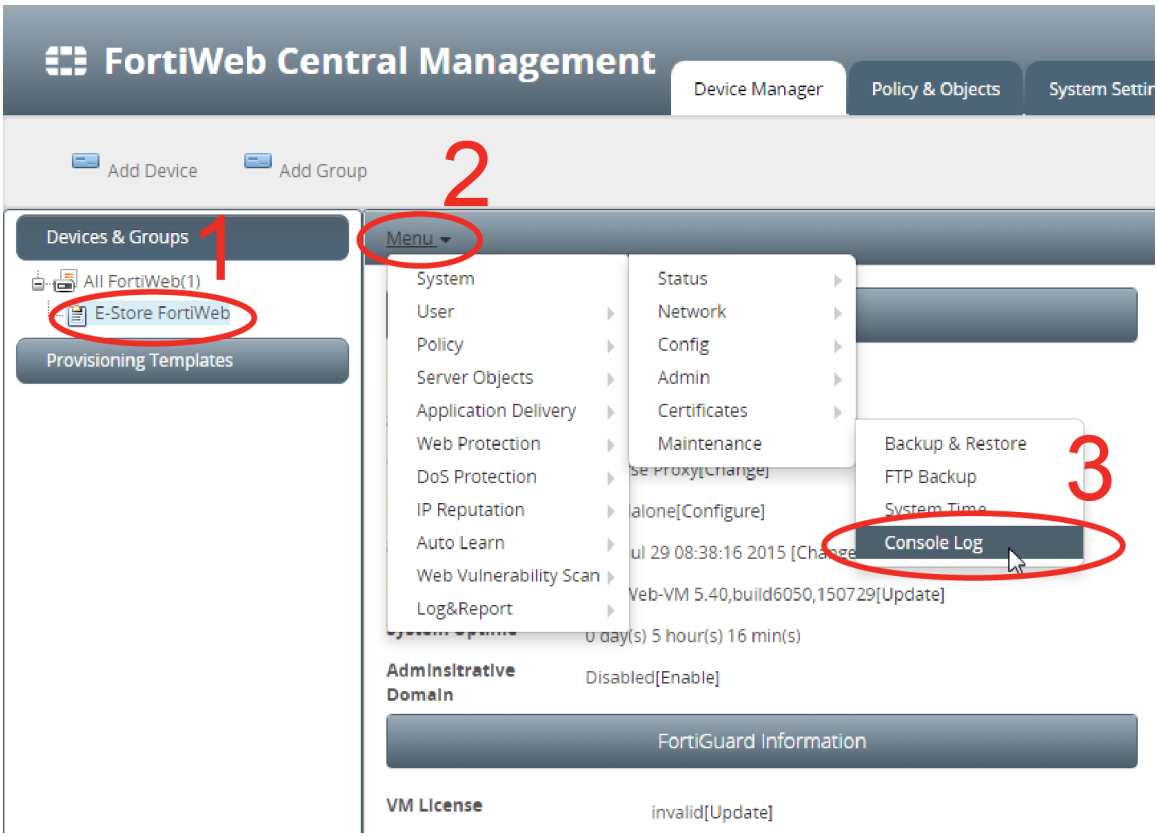
FortiWeb Manager applies any changes you make to the device configuration immediately. And if another administrator makes changes to the device you are viewing, FortiWeb Manager displays those changes the next time it refreshes the view (for example, when you select a different configuration element.)

To access individual configuration settings for a device

1. Under **Devices & Groups**, expand the **All FortiWeb** item.
2. In the list of devices, click the appropriate device.

   By default, the content pane displays the status dashboard for the device.

3. In the content pane toolbar, click **Menu**, and then use the menu to select the configuration item you want to view or edit.



Creating and applying provisioning templates

The **Provisioning Templates** navigation menu allows you to add, edit, and apply sets of settings that you use when you initially set up a FortiWeb.

You can edit a template at any time, but FortiWeb Manager does not apply the changes to a device until you apply or reapply the template.

To apply the template settings to a FortiWeb, you first use the **Add Device** option to add it to the device list.

When you apply a template to a device, FortiWeb Manager saves the current system configuration values. If it is unable to apply one or more settings from the template, it restores the values it saved. If successfully applies the template, it saves the original values as a file you can download or restore using the Templates Assign log (see Templates Assign on page 25).

For descriptions of the template configuration settings, see the *FortiWeb Administration Guide*.

Task	Instructions
Create a new system template	1. Under **Provisioning Templates**, right-click any item, and then click **Create New**. 2. Enter a name and optional description, and then click **OK**. 3. For each widget, enter appropriate values, and then click **Apply**. **Apply** saves values in the template. To apply it to a device, you apply the template to the device.
Add or update settings in the template	Under **Provisioning Templates**, click the appropriate template, add or edit settings in the appropriate widget, and then click **Apply**.
Apply system template settings to a FortiWeb	1. Under **Provisioning Templates**, right-click the template, then click **Assign Device**. 2. For **Devices**, select the device you want to apply the template to, and then click **OK**.
Delete a system template	Under **Provisioning Templates**, right-click the template, then click **Delete**.
Revert to the original configuration	Go to **Logs > Template Assign**, and for the log item for the template assignment, click **Revert**. For more information, see Templates Assign on page 25.

Upgrading a device group

You can use uploaded firmware and data analytics definitions files to upgrade all FortiWeb appliances in a group in a single operation.

Before you upgrade using FortiWeb Manager, ensure that the device or devices you want to upgrade are part of a group. (A group can contain a single device.)

When it upgrades a gateway, FortiWeb Manager attempts to update the gateway configuration to match the features of the newer firmware version. It deletes configurations that it cannot successfully update.

You cannot use the FortiWeb Manager web UI to downgrade device firmware.

Task	Instructions
Upload firmware	1. On the Device Manager tab, click **Firmware**. 2. Click **Import**. 3. Enter a name for the firmware, click **Choose File** to navigate to and select the firmware file, and then click **OK**.
Upload data analytics definitions	1. On the Device Manager tab, click **Data Analytics**. 2. Click **Import**. 3. Enter a name for the definitions, click **Choose File** to navigate to and select the definitions file, and then click **OK**.
Upgrade a device group	1. On the Device Manager tab, in the Devices & Groups tree, right-click the group to upgrade, and then click **Upgrade**. 2. Select **Firmware** or **Data Analytics**. 3. For **Firmware** or **Data Analytics**, select the file you uploaded earlier. 4. Click **OK**.

Create and install reusable server policies (Policy & Objects tab)

The **Policy & Objects** tab allows you to create, manage and apply the following reusable configuration resources:

- Shared configuration objects such as virtual servers, server pools, and web protection profiles. Server policies in packages reference these objects in server policies, either directly or through other objects. You can reference each configuration object in multiple policies and objects. You can't delete an object if it is referenced by a policy or another object.
- Policy packages that contain one or more server policies and apply to a specified operating mode. Thses server policies use the predefined configuration objects.

Package installation

When your policy package is complete, you can install it on a FortiWeb from the FortiWeb Manager device list. For each policy package, FortiWeb Manager maintains a list of the installation instances.

When you install a policy package on a device, FortiWeb Manager saves the current values of all server policies and related objects on the target appliance. If FortiWeb Manager successfully installs the package, it saves the original configuration as a file you can download or restore using the Package Install log (see Package Install on page 25). If the installation is unsuccessful, it restores the values it saved.

FortiWeb Manager only installs the reusable configuration objects that are referenced by policies in the package. However, to avoid possible conflicts, it deletes all configuration objects from the target FortiWeb, even if they are not referenced by a policy.

Editing packages

You can edit a policy package at any time, but FortiWeb Manager does not apply the changes until you install or reinstall the package.

Task	Instructions
Create configuration objects	1. On the Policy & Objects tab, under **Objects**, expand the navigation tree items until the type of object you want to create is displayed, and then click it. 2. In the content pane, click **Create New**. 3. Complete the settings for the new object, and then click **OK**.

Task	Instructions
Create a new policy package	1. Click **Policy Package > Create New**. 2. Enter a name for the package, select an operating mode, and then click **Apply**.
Add a policy to a policy package	1. Ensure that you have added the configuration objects that the policy uses to the list of objects. 2. Under **Policy Package**, select the package to add the policy to. 3. In the Policy & Objects toolbar, click **Policy > Create New**. 4. Complete the settings for the policy, and then click **Apply**.
Install a policy package on a FortiWeb	1. Under **Policy Package**, right-click the package to install, and then click **Install Wizard**. 2. Select the appropriate device, enter an optional comment, and then **OK**.
Revert to the original configuration	Go to **Logs > Package Install**, and for the package installation log item, click **Revert**. For more information, see Package Install on page 25.

High Performance Network Security